UDC 004.056 : 378.14

[1]Y. Baryshev
[2]N. Hands

FACILITATING STUDENT LEARNING OF CYBERSECURITY: ADAPTING US EXPERIENCE

[1]Vinnytsia National Technical University
[2]Purdue University

Анотація

Представлено аналіз методик викладання кібербезпеки в університетах США на основі досвіду Purdue University. Розглянуто моделі освітнього процесу. Виділено важливі аспекти для покращення викладання дисциплін та описано досвід їх впровадження на кафедрі захисту інформації ВНТУ.

Ключові слова: кібербезпека, педагогіка, контроль знань.

Abstract

The cyber security teaching methodology at US universities using Purdue University's experience analysis is presented. Educational models are shown. The essential aspects of curriculum learning improving are determined and their integration experience at VNTU's information protection department is described.

Keywords: cybersecurity, pedagogic, assessments.

Introduction

Ukrainian educational system is in the middle of changes from post-Soviet educational model towards "western" model that is caused by both Ukraine's integration to EU and rationality. The need of changes in the field of cyber security is even more dire – recent state of Ukrainian foreign relations make it one of the world's hottest information warfare spots. At the same time one of the most successful and developed educational models according to number of Nobel prizes winners [1] is USA's educational system. Therefore, it should be carefully analyzed and the factors making the difference are to be integrated within Ukrainian universities, such as Vinnytsia National Technical University (VNTU) which providing cyber security curricula for students over last 20 years. Purdue University's cybersecurity program is considered as one of the USA's most advanced [2]. Moreover, Computer and Information Technology Department of Purdue University is one of the world oldest departments dedicated IT teaching and as such having the biggest experience in the field. Therefore, the experience and models must be adapted to VNTU's curricula in order to perform abovementioned educational model transformations.

The goal of this research is to facilitate cybersecurity teaching using the respective experience used at Purdue University.

Research results

Bare curriculum changes won't produce results without teaching methods alterations and students adaptation to these methods. Consequently, the teacher-student relations and tasks of both counterparties are as important as courses content. The most intense cooperation between them appeared during the laboratory and practical works as well as during knowledge assessments, where students play active role. According to Purdue University's experience the most productive is constructivist's approach, where students are opening the field of knowledge by themselves and teacher playing role as a guide. This allows reaching deeper students involvement into the studying process. When student passively involved the transition between different ideas might be considered as kind of magic or just as given things. While they actively seeking the answers taking the paths of these ideas inventors did – they are able to experience the feeling of wonder those is present for any inventing activity and the building the picture of the area by themselves, so they would see if some peace of knowledge is lacking and desiring to find it collaborating as a team with each other and a faculty members. As a result students gain solid ground of the knowledge and develop soft skills those are needed in almost any field of future work [3].

Another important aspect of studying is adoption of Bloom's taxonomy and its revisions [4] according to

which some kinds of thinking activities are mo complex than others. The revision [4] states them in the following order: remember; understand; apply; analyze; evaluate; create.

The exact order is quite discussable topic, but the idea that remembering is not meaning understanding, and respectively understanding doesn't mean the ability to apply the knowledge not mentioning multiplying them is obvious and need to be considered during practical tasks and assessments activities

Developing adversarial mindset is essential for performing cyber security specialist's job tasks, because by anticipation of adversary's future steps will help not only prevent malicious actions, but to uncover adversary identity. Honey pots planting is the example of such anticipation skills application.

Above mention steps were implemented during courses "Cyber Security Monitoring and Audit" [5, 6], "Software Development Security" of the master's curricula and some elements were integrated as a part of "Database Designing", "Operating Systems Protection" and "Specialized Processor-based Information Protection Systems" at bachelor's curricula at VNTU's information protection department for students studying 125 - Cybersecurity program. The result of integration shows increase in student involving and lectures attendance of master students.

Conclusion

The demands of reforming cyber security teaching methods caused need in international collaboration and this experience absorption. Pedagogical aspects covered in this report and essential for preparing cyber security specialist and they may be perceived to be quite obvious and simple to follow, but its implementation showed to be much trickier than it seemed. Their implementation needs a lot of planning to balance tasks difficulty and future jobs demands.

REFERENCES

1. All Nobel Prizes. URL: https://www.nobelprize.org/prizes/lists/all-nobel-prizes (accessed 05.03.2021)
2. Cybersecurity URL: https://polytechnic.purdue.edu/degrees/cybersecurity (accessed 05.03.2021)
3. K. Neubauer and others. Teamwork Makes the Dream Work: Purdue' s IMPACT Course Transformation Faculty Learning Community. Purdue University Purdue e-Pubs. 2018. URL: https://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1036&context=impactpres (accessed 05.03.2021)
4. David R. Krathwohl. A Revision of Bloom's Taxonomy: An Overview. Theory into Practice, Volume 41, Number 4, Autumn 2002. P. 212-218. URL: https://www.depauw.edu/files/resources/krathwohl.pdf (accessed 05.03.2021).
5. Yurii Baryshev and Olesia Voitovych. IT audit course development for cybersecurity curricula students using USA's methodology. "Інформаційні технології та комп'ютерне моделювання"; матеріали статей Міжнародної науково-практичної конференції, м. Івано-Франківськ, 18-22 травня 2020 року. Івано-Франківськ, п. Голіней О.М., 2020. С. 135-136 URL: http://itcm.comp-sc.if.ua/2020/zbirnyk2020.pdf (accessed 05.03.2021).
6. Y. Baryshev. Analysis of USA cybersecurity teaching methodology implementation at Vinnytsia National Technical University. Матеріали XLIX науково-технічної конференції підрозділів ВНТУ, Вінниця, 27-28 квітня 2020 р. URL: http://ir.lib.vntu.edu.ua/bitstream/handle/123456789/29416/9456.pdf?sequence=3 (accessed 05.03.2021).

Баришев Юрій Володимирович — к. т. н., доцент кафедри захисту інформації, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: yuriy.baryshev@vntu.edu.ua

Хендс Ніколь — провідний викладач з кібербезпеки, факультет комп'ютерних та інформаційних технологій, політехнічний інститут / Центр освіти та досліджень в галузі інформаційного забезпечення та безпеки (CERIAS), Університет Пердью, Вест-Лафайетт (Індіана, США), email: nhands@purdue.edu

Yurii Baryshev — PhD. (Eng), Associated professor of Information Protection Department, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : yuriy.baryshev@vntu.edu.ua

Nicole Hands — Clinical Assistant Professor of Cybersecurity, Computer and Information Technology Department, Polytechnic Institute / The Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University, West Lafayette (Indiana, USA), email: nhands@purdue.edu